The compatibility of decryption orders with the right against self-incrimination: compelled revelation of Passwords

Evangelos Vordoglou

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

LLM in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law

February 2016
Thessaloniki – Greece

Student Name: Evangelos Vordoglou

SID: 1104130034

Supervisor: Prof. Eleni Kosta

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February 2016

Thessaloniki – Greece

Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law at the International Hellenic University.

It focuses on compelled key decryption in light of the privilege against self-incrimination and is basically divided into two large chapters, the first one concerning the emergence of data encryption and decryption in technology as well as their treatment in legislation. The second one, which constitutes the main chapter of the dissertation is an attempt to analyze the legislation of certain states and the jurisprudence mainly of the European Court of Human Rights related to mandatory key disclosure in the light of the privilege against self-incrimination, that is examining the cases in which the above privilege protects individuals from the compulsion of the authorities to disclose or deliver certain information and data and more specifically to disclose the passwords that encrypt electronic data.

The support and guidance I received from my supervisor Prof. Eleni Kosta was decisive for my study of the educational material disposed to me and the final form of this dissertation, therefore I would like to express my gratitude for the honest interest and kind support. Moreover, I could never forget to acknowledge my Professor Dr. Athanassios Kaissis for continuously supporting me in person, with his assistance being not only moral but also practical when a year ago I was literally about to give up after an extremely severe health issue I faced and he inspired me to continue my studies, while he-along with the academic assistants and the University staff- exhausted every practical and procedural margin to help me resume my studies. Thus, I would like to thank them all deeply for helping me meet the demands of this paper.

Keywords: mandatory key disclosure, key decryption, data decryption, password decryption, right to silence, privilege against self-incrimination

Evangelos Vordoglou

14.02.2016

Preface

The purpose of this dissertation is to highlight the importance of the privilege against self-incrimination in protecting individuals from compelled decryption of incriminatory data. National and international legislation as well as jurisprudence, mainly of the European Court of Human Rights, form and regulate the specific characteristics of the privilege and the cases in which it applies. We shall see that even though the privilege, as well as the relative right to silence, is recognized as a fundamental part of the right to a fair trial numerous exemptions have been introduced to weaken its application.

This dissertation aims to be of particular interest to law students who focus on the study of human rights in criminal proceedings as it highlights one of the most significant legal tools in the protection of individuals against the omnipotence of the judicial authorities in the area of data decryption.

Contents

Introduction

The dissertation focuses on compelled revelation of passwords in the light of the privilege against self-incrimination. In order to understand the procedure as well as the role of data encryption and decryption in modern society the first part of chapter one describes briefly the meaning of the two notions. The second part includes a reference to the legal treatment of both encryption and decryption in a national level as well as within the legal orders of certain countries. The aim of this reference is to highlight the legal importance of encryption as a means of ensuring privacy and that of decryption as part of the criminal proceedings in obtaining evidence that concern an offence.

The second chapter is the core of the dissertation as it examines compelled password decryption in the light of the privilege against self-incrimination. The first part constitutes a brief historical overview of the privilege as well as a reference to the right to silence and the difference between the

two notions. In the second part of the chapter we examine mandatory key disclosure within certain legal orders and, more specifically, the conditions under which these legal orders provide compelled revelation of passwords. At the same time, we examine the legal provisions within these legal orders that guarantee the protection of human rights, and more specifically that of the privilege against self-incrimination, during the criminal proceedings that concern mandatory key disclosure. The aim of this analysis is to discover the legal tools provided in international and national legislations for the suspect and/or witness so as not to produce passwords that may reveal self-incriminating information. The privilege against self-incrimination constitutes thus a fundamental right for the person charged with a crime which protects him against the omnipotence of the state, the investigatory and judicial bodies and a significant aspect of the right to a fair trial. The third part of the chapter concerns the jurisprudential treatment of mandatory key disclosure, consisting of a selection of cases that have played an important role in forming in practice the privilege against self-incrimination with regard to compelled password decryption.

The last chapter of the dissertation consists of a comparative analysis firstly of the legal orders mentioned in the previous chapter in order to understand the differences as well as the similarities of certain legal orders on the issue. The comparison of the jurisprudential trends that follows in the next part aims to clarify certain significant conclusions reached in the examined cases in order for us to acquire an overall view of the issue under discussion. The third part aims to make an assessment of the material that collected and examined in the previous chapter with a view to highlight the importance of the privilege against self-incrimination.

Finally, we cite the conclusions we reached in this dissertation as well as the bibliography on which it is based.

Chapter 1: Data encryption and data decryption – with specialization on passwords

Data encryption and data decryption – with specification on passwords – describe the two contradictory sides of modern cryptology, that is, in a more general concept, the "technology that, if good enough, can blocks access to files in storage or in transit" (Kahn D. 1996:983). In this chapter we are going to discuss both the basic characteristics of this technology and its legal treatment within the international law and a number of legal orders of European and other countries.

1.1. What is data encryption and decryption?

Data encryption and data decryption are part of the technology concerning the production of encrypted documents and files by numerical and/or alphabetical passwords, or even nowadays of other personal information such as fingerprints and DNA, that are either memorized or saved by their owner with a view to prevent unauthorized access to them and thus ensuring computer security. More specifically with reference to the exchange of electronic messages "mathematical algorithms are used to scramble information for future recovery. Specifically, the unscrambled 'plaintext' is converted into a 'ciphertext,' or a series of apparently random characters. With the use of a 'key' known only to the intended recipient of the message, the 'ciphertext' is converted back into 'plaintext' (Rueda A. 2001:17). As a result, "passwords can be encrypted so that they cannot be read even if the file in

which they are stored is accessed" (Kahn D., *idem*).

The need for the production of encrypted data in our society, greatly characterized by the advances in technology, is quite obvious. Computers are increasingly used not only as a means of communication but also as a means of files storage. At the same time, modern technology jeopardizes permanently the privacy of our communication, in an interpersonal as well as in a professional level, as unauthorized accessibility to files and documents has become incredibly easy. Personal information and secrets but also personal data held by certain professions such as doctors and lawyers and certainly economic information concerning institutions and private companies are but secured unless measures are taken. Thus "[I]t is essential for certain transactions to be encoded to prevent their interception or fraudulent alteration. This issue is of critical importance to the computer and banking industries, as well as the overall American economy" (Mandelman J. C. 1998:236-37) and we would add, for the overall global economy. In this double role of modern technology and its possibilities a matter of security arises as well as a matter of protection of privacy and human rights and it is precisely at the antipode of this insecurity that data encryption has attempted to give a solution. As it has been aptly noted "modern technology briefly took away privacy, but subsequently recreated it" (Clemens A. M. 2004:4). All the above do not exclude the possibility that encryption technology may also be – and is indeed sometimes – used for criminal purposes. And this area is precisely the subject of the present paper.

Data decryption constitutes the response of technology to data encryption, which is the use of cryptological means in order to gain access to encrypted documents and files, and within this paper's context, the main tool in the enforcement authorities' hands with reference to gathering evidence in criminal proceedings. Thus, the enforcement authorities shall use for instance experts in order to try to decode passwords and decrypt the files of interest in a particular case but, as we shall see in the next chapters, sometimes the acquirement of passwords and access to certain files and documents can only be achieved with the cooperation of the suspect or a certain witness. In these cases "the government can subpoena a person to testify before a grand jury and bring the private key and/or a decrypted version of a seized message. The government can thereby compel decryption or the production of the private keys that will decrypt an encrypted message, unless the person exercises a valid privilege" (*Ibid*, 2004:5).

1.2. Legal treatment of the phenomenon

As we mentioned above data encryption and data decryption interest the criminal law insofar as they are involved in the criminal proceedings of gathering evidence about a case. Thus in this chapter we shall examine in brief their treatment within the international law as well as the legal orders of certain European and other countries.

1.2.1. International law

With reference to the international regulation of cryptography and the protection or encryption of important data and information there are several international treaties and acts. For instance, the Wassenaar Arrangement is a multilateral export control regime where the import and export of data encryption, as a dual-use technology – that is as both a commercial and military good – are based on certain agreed principles (Saper N. 2013:678). Also, the Recommendation of the Council concerning Guidelines for Cryptographic Policy of the OECD, released on March 1997 sets out a out a generous framework for encryption policies and stresses "the importance of the availability and choice of strong encryption products subject to proportionate and effective measures to safeguard law enforcement needs" (Andrews S. 2000).

Furthermore, in the economic sphere and the protection of relevant information we find numerous acts such as the PCI DSS (Payment Card Industry Data Security Standard) concerning the protection of payment card data and related consumer/business details during processing, transmission, and storage as well as the International Basel II Accord which focuses on international standard for operational and financial risk management for banking institutions and provides "mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing must become part of the data's lifecycle" (Shackleford D. 2007:9). Finally, with reference to the health section, the HIPAA (Health Insurance Portability & Accountability Act) concerns the protection of electronic patient healthcare data and information.

Within the European Union legislation the EURO-SOX focuses on the protection of sensitive data related to financial reporting in public and the 95/46/EC EU Directive regulates the general protection

of individual's private information. It is noteworthy that the EU institutions have always supported the "free domestic use of strong cryptography […] Hence, European support for the free use of encryption and opposition to mandatory key escrow proved critical to the continued development of strong cryptography" (Saper N. 2013:682).

On the other hand, provisions about offenses that are related to computers and/or data decryption are found in several international treaties. Thus, the CCC (Convention on Cybercrime)[1] Art. 19 subsection 4 "enables law enforcement officers to order a person who has knowledge about the functioning of a computer system or about the security measure against illegal access of the system or in order to protect the confidentiality of the data content, to provide the information to law enforcement necessary to access the data and secure it" (Kaspersen H. W. K. 2004:92). That is to say that "the investigating authorities may apply any measure to assure the access to the computer system, including technical means and hacking tools" (*Idem*). However, international law as well as national legal orders provide specific restrictions and safeguards to this access, which we are further examining in the next chapter. Other examples of international and regional agreements concerning offenses that relate to data decryption include the League of Arab States Convention and the COMESA Draft Model Bill[2].

1 Drawn up by the Council of Europe, it was signed in Budapest on November 23, 2001 and entered into force on July 1st, 2004.

2 Comprehensive Study on Cybercrime, Draft-February 2013, United Nations Office On Drugs and Crime. p. 198

1.2.2. Legal orders of European and other countries

With reference to legal orders of European and other countries concerning the regulation of data encryption the US GLBA (GRAMM-LEACH-BLILEY-ACT) focuses on the protection of private data in the financial services industry while the SB 1386 (California Senate Bill 1386) refers to the general information of personal data. The Japanese Financial Instruments and Exchange Law of 2006 focuses on the protection of sensitive data related to financial reporting in public and the PIPLE (Personal Information Protection Law) of 2003 on the protection of the privacy of personal consumer data. Finally, Canada's PIPEDA (Personal Information Protection & Electronic Documents Act) refers to the protection of personal and private data under certain circumstances. In Europe, Germany's BDSG (BUNDES-DATENSCHUTZ-GESETZ) refers to the general protection of an individual's private information and UK's DPA (Data Protection Act) of 1984 (amended in 1998) refers to the general handling of personal information[3].

What is of more interest though within this paper is the regulation of mandatory key disclosure or compelled decryption, or else the mandatory decryption of the passwords[4] preventing access to unauthorized access, within a number of legal orders of European and other countries. To begin with, in Belgium the Art. 9 §§ 1, 2 and 3 Law on computer crime of 28 November 2000[5] provides that the

---

3 Shackleford D., *Regulations and Standards: Where Encryption Applies*, SANS Institute InfoSec Reading Room, November 2007

4 It is important to note that there is a significant difference between compelled key disclosure and compelled data decryption. The first one constitutes a greater intrusion into a person's privacy as "compelling production of a private key would facilitate decryption of any and all communications encrypted with this private key, even those documents whose existence has not been proven. A person will likely often use one public/private key set to encrypt all her communications. Therefore, compelling private key disclosure can never be equivalent to compelled document decryption". (Clemens A. M. 2008, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, Computer Crime Seminar Georgetown University Law Center Professors Richard Salgado 3 & Christian Genetski, p. 17)

5 http://cwisdb.kuleuven.be/pisa/fr/jur/infocrimewet.htm : " Art. 88quater. § 1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible.
§ 2. […] L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.

investigative judge or a prosecutor's assistant police officer delegated by him may order a person presumed to have special knowledge of the computer system which is the subject of the specific research or of the services that protect or encrypt data that is stored, processed or transmitted by a computer system, to provide information on the functioning of the system and the ways to access or to directly access data that is stored, processed or transmitted by such a computer system into a comprehensible form. Also, the person who refuses to provide such an assistance or who impedes such an access is punishable with imprisonment from six months to one year and/or a fine from 26 to 20 thousand francs. However, according to paragraph 2 of the above article, the people referred to in Art. 156 as well as the person who is charged with a crime in the particular case are exempted from the above provision.

In UK the Regulation of Investigatory Powers Act 2000 Part 3 (RIPA III) about the investigation of electronic data protected by encryption concerning the power to require disclosure provides that "49(3) A disclosure requirement in respected of any protected information is necessary on grounds falling within this subsection if it is necessary – (a) in the interests of national security; (b) for the purpose of preventing or detecting crime; or (c) in the interests of the economic well-bring of United Kingdom"[6]. The next articles of the Act describe in detail the procedure that has to be followed in this case.

Concerning the regulation of compelled decryption in Australia the Cybercrime Bill 2001 of the Parliament of the Commonwealth of Australia, schedule 2 item 12 provides that "This Item inserts proposed new sections 3LA and 3LB into the Crimes Act. Proposed section 3LA would enable a law enforcement officer executing a search warrant to apply to a magistrate for an 'assistance' order. To grant the order, the magistrate would have to be satisfied (i) of the existence of reasonable grounds to suspect a computer on search premises contains evidence of an offense; (ii) that the subject of the order is reasonably suspected of the offense or is the owner of the computer or computer system, or a current employee of the owner; and (iii) that the subject of the order has relevant knowledge of the

§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement»

6 See the document in http://www.legislation.gov.uk/ukpga/2000/23/part/III

functioning of the computer or system or measures applied to protect the computer or system.

The person to whom the order is directed would be required to provide the officer, to the extent reasonably practicable, with such information or assistance as is necessary to enable the officer to access data on the computer system, copy it to a storage device or convert it to documentary form. For example, a person could be required to explain how to access the system or to provide a password to enable access. The maximum penalty for non-compliance with the order would be 6 months imprisonment"[7].

Finally, in France Law 2001-1063 about everyday security entered in force in 15 November 2001 (Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne). Chapter IV of the above law provided changes in the Law 1991-646 (Article 11-1), in the Code of Criminal Procedure (Article 230-1 and Article 706-71) as well as in the Penal Code (Article 434-15-2)[8], which we are examining in the next chapter, so that a justice either prosecuting attorney may force whatever officially recognized individual to decode either yield keys to create accessible encrypted data that ran into in the program of an examination.

7 See the document in http://www.austlii.edu.au/au/legis/cth/bill_em/cb2001122/memo1.html

8 See the document in http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052

CHAPTER 2: The right against self-incrimination

We have seen in the previous chapter that national legal orders as well as international treaties protect encrypted data as they are regarded of significant importance both for the smooth operation of the economy and the security of privacy. On the other hand mandatory key disclosure consists an equally important part of the criminal legislation as part of the criminal procedure in the investigation of offenses related somehow to computers and data stored in them. In this chapter we are examining the right against self-incrimination as a legal tool that restricts mandatory key disclosure.

2.1. Historical overview

The right against self-incrimination – as well as the relative right of silence – is not included in Art. 6 of the European Convention on Human Rights of 1950 (ECHR) which deals with the general right to a fair trial but, as we shall see, it has been implied into the above article in various judgments on the fairness of criminal trials and it was first recognized in 1993 in the case Funke v. France, which we are going to examine in detail. On the other hand, Art. 14(3)(g) of the U.N.'s International Covenant on Civil and Political Rights of 1966 (ICCPR) explicitly provides that "3. In the determination of any criminal charge[9] against him, everyone shall be entitled to the following minimum guarantees, in full equality: […] g. Not to be compelled to testify against himself or to confess guilt". It is noteworthy that the ECHR does not include an explicit reference to the right against self-incrimination but according to Trechsel (2005:340) "the absence of a corresponding guarantee is justified by the fact that it was agreed that the right formed part of the general fair-trial guarantee".

The privilege[10] is also recognized in the Art. 8(2) (g) of the American Convention on Human

9 Trechsel S. (2005), *Human Rights in Criminal Proceedings*, Oxford University Press, p. 155: "The reference to the "charge" can be explained by pointing out that persons against whom criminal proceedings are brought are particularly vulnerable as far as this presumption [of guilt] goes; they need protection against the eagerness of prosecutors who will tend to anticipate their own success and treat or present the suspect as guilty".

10 *Ibid*, p. 341 "What is meant is the right not to be *compelled* to incriminate oneself, to be protected against any

Rights of 1969 (ACHR) according to which "[...] During the proceedings, every person is entitled, with full equality, to the following minimum guarantees: (g) the right not to be compelled to be a witness against himself or to plead guilty; 3. A confession of guilt by the accused shall be valid only if it is made without coercion of any kind" as well as numerous national legal orders.

The privilege, as we shall see, is closely related to the presumption of innocence, which is one of the fundamental rights introduced for the protection of the individual against the possible arbitrariness of justice and the power of the state apparatus. The presumption of innocence thus "must be regarded as a guiding principle which exists in order to regulate the treatment of persons who have not yet been convicted. Such people must be dealt with in a way that is compatible with the possibility that they are innocent. Two types of behavior vis-à-vis a suspect can be distinguished: factual and verbal. No measure may be taken, no restriction imposed which implies the guilt of the suspect. Further, declarations that a suspect is guilty of an offence are forbidden" (Trechsel S. 2005:156).

Finally, it is of great importance to make a distinction between two rights that are often regarded to have an identical content, that is the distinction between the privilege against self-incrimination and the right to remain silent[11]. As it is noted, however, "the two guarantees must be seen as being represented by two partly overlapping circles. The right to silence is narrower in that it refers to acoustic communication alone, the right not to speak. The privilege goes further in that it is not limited to verbal expression. On the other hand, the scope of the right to silence goes beyond that of the privilege as it does not protect against the pressure to make statements detrimental to the person concerned, but any declaration at all" (*Ibid*. 2005:342).

pressure to make a statement. I have opted for the term "privilege" short for "privilege against self-incrimination" because it refers to the situation of someone who enjoys enhanced protection".

11 Hocking B. A. and Manville L. L. (2001), *What of the right to silence: Still supporting the presumption of innocence, or a growing legal fiction?*, Macquarie Law Journal (2001) Vol 1 No 1, p. 65 where the right to silence "is a procedural protection for the individual against the power of the State with origins in revolutionary times following the overthrow of the remains of clerical and monarchical absolutism in the middle of the 17th century".

2.2. Data decryption in the light of the right against self-incrimination in European and other countries

In this subsection we are examining the data decryption in the light of the right against self-incrimination in several European Countries, that is in UK, France, Belgium, Netherlands and finally in Australia, while we are siting some information about the US.

2.2.1. UK legal order

As we mentioned above, in UK data decryption falls within the Regulation of Investigatory Powers Act 2000 Part 3 (RIPA III), while the privilege against self-incrimination is provided in s. 14(1) of the Civil Evidence Act 1968.

First of all, this section of the above Act, under the title *Investigation of electronic data protected by encryption etc.*, applies where protected information has come into the possession of any person "by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property" [s.49(1)(a)] or "by means of the exercise of any statutory power to intercept communications" [s.49(1)(b)] or "by means of the exercise of any power conferred by an authorisation under section 22(3) or under Part II, or as a result of the giving of a notice under section 22(4)", where section 22(3) refers to "the designated person [for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data] may grant an authorisation for persons holding offices, ranks or positions with the same relevant public authority as the designated person to engage in any conduct to which this Chapter applies", Part II concerns the *Surveillance and covert human intelligence sources* and section 22(4) refers to the case in which "the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator" to obtain or disclosure all that data that is in his possession or that was subsequently obtained by him [s.49(1)(c). Or "as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information)" [s.49(1)(d) or "has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or Her Majesty's Revenue and Customs. Next, s.49(2)(3) and (4) provides the conditions that

have to be respected in order for the person with the permission under Schedule 2 to impose a disclosure requirement in respect of the protected information by notice to the person whom he believes to have possession of the key and s.49 subsections (5) to (9) concern special cases about the person to whom a notice for key disclosure must be given or about the disclosure of certain keys.

With reference to the obligations imposed to the person who is believed by the designated person to be "in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form" [s.50(1)] and thus is given the above notice, he is obliged "to make a disclosure of any information in an intelligible form shall be taken to have complied with that requirement if—(a) he makes, instead, a disclosure of any key to the protected information that is in his possession; and (b) that disclosure is made, in accordance with the note imposing the requirement, to the person to whom, and by the time by which, he was required to provide the information in that form [s.50(2)].

Concerning the safeguards provided by the law against compelled decryption in s.51(4) and (5) as well as in s.55, the privilege against self-incrimination does not appear in any of them. However, the right is explicitly provided in section 14(1) of the Civil Evidence Act 1968[12] under the title *Privilege against incrimination of self and spouse* according to which "The right of a person in any legal proceedings other than criminal proceedings to refuse to answer any question or produce any document or thing if to do so would tend to expose that person to proceedings for an offence or for the recovery of a penalty—(a) shall apply only as regards criminal offences under the law of any part of the United Kingdom and penalties provided for by such law; and (b) shall include a like right to refuse to answer any question or produce any document or thing if to do so would tend to expose the spouse or civil partner of that person to proceedings for any such criminal offence or for the recovery of any such penalty'. The section further provides that (4) Where any existing enactment (however worded) that— (a) confers powers of inspection or investigation; or (b) provides as mentioned in subsection (3) above, further provides (in whatever words) that any answer or evidence given by a person shall not be admissible in evidence against that person in any proceedings or class of proceedings (however described, and whether criminal or not), that enactment shall be construed as providing also that any answer or evidence given by that person shall not be admissible in evidence against the husband or wife of that person in the proceedings or class of proceedings in question".

12 See the document in http://www.legislation.gov.uk/ukpga/1968/64/section/14

Thus, according to the above section the dual protection of the person consists on the one hand that any person can refuse to answer any question or produce any document, if to do so would "tend to expose" that person to proceedings for a criminal offence or criminal penalty and also that "any answer or evidence given by a person shall not be admissible in evidence against that person in any proceedings or class of proceedings". Moreover, the privilege applies to the UK through its implication in Art. 6 of the ECHR as incorporated into English law by the Human Rights Act 1998.

Finally, certain exceptions from the privilege have been established both by the courts and by laws such as s13 of the Fraud Act 2006[13] according to which (1) A person is not to be excused from— (a) answering any question put to him in proceedings relating to property, or (b) complying with any order made in proceedings relating to property, on the ground that doing so may incriminate him or his spouse or civil partner of an offence under this Act or a related offence. Yet the above statement or admission is not admissible in evidence against him or his spouse or civil partner [s. 13(2)].

2.2.2. France legal order

We have already seen that in France Law 2001-1063 about everyday security introduced several significant modifications in the legislation related to mandatory key disclosure. Thus, Article 11-1 of the above law provides that natural or legal persons providing cryptology services to ensure privacy are required to submit to officials authorized in accordance with Article 4, at their request, keys allowing decryption of data processed through the services provided by them. Authorized officials may ask the aforementioned service providers to implement these keys themselves unless they show that they are not able to meet these requisitions. In case the above mentioned services do not comprise with these requirements, they are punishable by two years of imprisonment and a 30,000 euro fine.

Furthermore, according to Art. 434-15-2 of the Penal Code any person who has knowledge of the secret decryption key of a means of cryptology that may have been used to prepare, facilitate or commit a crime or an offense and refuses to either deliver this key to the judicial authorities or to use it at the suit of the authorities mentioned in the Article, is punishable by three years of imprisonment

13 See the document in http://www.legislation.gov.uk/ukpga/2006/35/section/13

and a 45,000 euro fine.

Finally, according to Art. 230-1 of the Code of Criminal Procedure, which was also introduced by law 2001-1062, in cases where it appears that data seized or obtained during the investigation or trial have undergone processing operations which prevent plain access to the information they contain or make them impossible to understand, the prosecutor of the Republic, the investigating court or the trial court dealing with the case may appoint any person or qualified corporation, to carry out technical operations to obtain either the plaintext version of this information or, if a means of encryption was used, the secret decryption key, if it appears necessary. However, the Article provides also that all the above apply "without prejudice to the provisions of Articles 60, 77-1 and 156", which refer to the persons designated to provide the technical support, that may be any qualified person or expert.

The privilege against self-incrimination is implied in Art. 63-1 of the Code of Criminal Procedure. The above article was introduced by Art. 7 of the Law 2000-516 with a view to reinforce the protection of the presumption of innocence and the rights of the victims and was later modified in a more subtle form by Art. 4 of the Law 2014-535. In its first form the article provided that "the person in custody is immediately informed of their right not to answer to questions posed to him by investigators". Since its modification the article provides that the person in custody is immediately informed in a language that he comprehends that he has the right, during the hearings and after he has provided his identity, either to answer to the questions posed to him or to remain silent.

Thus the privilege against self-incrimination does not explicitly constitute a right within French legislation and it is solely implied within the right to remain silent and the principle of the presumption of innocence[14]. However, as we have seen the privilege against self-incrimination is not identified with the right to remain silence, as the latter provides the individual with the right not to answer at all to questioned posed to him, nevertheless it is more narrow than the privilege against self-incrimination, as it only includes acoustical communication and thus leaves the person unprotected to the pressures made by the authorities to provide other evidence, apart from verbal expression,

14 Hocking B. A. and Manville L. L. (2001), *What of the right to silence: Still supporting the presumption of innocence, or a growing legal fiction?*, Macquarie Law Journal (2001) Vol 1 No 1, p. 65: "The presumption of innocence "has been constructed so as to require the prosecution to prove guilt. In theory then, the criminal justice system should not tolerate methods of 'compulsory interrogation' such as those once associated with the Star Chamber".

which might incriminate him. This void in French legislation is filled with the application of Art. 6 of the ECHR which implies within its principle of a fair trial the privilege against self-incrimination.

2.2.3. Belgium legal order

We have already mentioned that in Belgium the legal provisions concerning compelled decryption are included in Law of 28 November 2000 about Cybercrime. More specifically, art. 9 modified article 88quater of the Code of Criminal Procedure as follows. According to the modified art. 88quater § 1er the investigating judge or an auxiliary police officer of the prosecutor's King delegated by him may order persons presumed by him to have special knowledge of the computer system that is the subject of research or of the services that enable the protection or encryption of data that is stored, processed or transmitted by a computer system to provide information on the functioning of this system and on the ways to access or to directly access data that is stored, processed or transmitted by such a system, in a comprehensible form. The judge mentions the circumstances of the case that justify the measure in a reasoned order that he sends to the prosecutor. Paragraph 3 of the same article provides imprisonment from six months to a year and a fine from 26 francs to 20,000 francs for the person mentioned above that refuses to collaborate with the authorities or is willing to prevent the research on the computer system.

Paragraph 2 of the above article provides that the aforementioned person may be any qualified one with the exemption of the people referred to in Art. 156 of the Code of Criminal Proceedings as well as the person who is charged with a crime in the particular case. Thus, Belgium legislation does not mention explicitly the right to remain silent or the privilege against self-incrimination, yet expressly forbids the authorities to force the person who is charged with an offense to cooperate with the authorities and thus give incriminating evidence for themselves. In this way, the person is protected from mandatory key disclosure of data that is stored in computers.

2.2.4. Netherlands legal order

Decryption obligation was introduced in Netherlands in the Computer Crime Act in 1993. At present art. 125K section 2 of the Dutch Code of Criminal Procedure provides that in case encrypted information is found in a computer during the house search[15] described in article 125i CCP "an order can be given to provide access of a secured computer and/or to decrypt relevant data" (Kooijmans T. & Mevis P. 2013:9). The order may be given to any person who can reasonably be supposed to know the means of encryption to decrypt the information with the exemption of the suspected person (art. 125k par. 3). Furthermore, the command to decrypt data can be given to anyone with the exemption of the suspected person[16] in case encrypted information is found in data delivered to the police on the basis of data-delivery orders according to art. 126nc-nf, 126uc-uf and 126zk-zn of the DCCP as well as art. 126nh, 126uh and 126zp of the DCCP[17].

Thus, legislation in Netherlands with reference to decryption obligation respect the privilege against self-incrimination as "to date the Dutch legislator has proceeded on the assumption that compelled decryption violates the privilege against self-incrimination (known in Dutch as the

15 As Koops B. J. notices in *Cybercrime Legislation in the Netherlands*, Electronic Journal of Comparative Law, vol. 14.3 (December 2010), p. 18 "These orders could initially be given *while* the officer conducted a search or network search, which was felt to be too restrictive, since often computers are seized and investigated at the office only some time *after* the search. Therefore, the formulation was adapted in the Computer Crime II Act, but for some reason or other the legislator replaced 'during a search' with 'when Article 125i or Article 125j has been applied'. [...] This implies that security-undoing or decryption orders cannot be given for computers or data carriers seized during normal searches. This was undoubtedly not the intention of the legislator, but the clear wording of Article 125k hardly allows for an analogous, teleological interpretation to cover other forms of searches. Moreover, it does not cover other situations in which computers are seized, for example when someone is stopped or arrested on the street and her laptop or pda is seized; this gap already existed under the old Computer Crime Act legislation, but has so far not been addressed by the legislator".

16 *Ibid*, p. 17 "The orders can be given to people who process the data in a professional capacity; an order of 'other' stored data and of sensitive data, however, can also be directed at people who process data for personal use. Suspects cannot, however, be ordered to provide data, in view of the privilege against self-incrimination. If the data are encrypted, the people targeted by the production order – excluding suspects – can be ordered to decrypt them, according to Article 126nh DCCP".

17 Koops B.J. http://www.cryptolaw.org/cls2.htm

principle of *nemo tenetur*)"[18].

2.2.5. Australian legal order

We have already mentioned that in Australian legislation compelled decryption is regulated in Cybercrime Bill 2001 of the Parliament of the Commonwealth of Australia. According to Item 12 of the above law, which inserts section 3LA in the Crimes Act 1914, "(1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following: (a) access data held in, or accessible from, a computer that is on warrant premises; (b) copy the data to a data storage device; (c) convert the data into documentary form". The next paragraph of the section provides that in order to grant the order, the magistrate asserts that "(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and (b) the specified person is: (i) reasonably suspected of having committed the offence stated in the relevant warrant; or (ii) the owner or lessee of the computer; or (iii) an employee of the owner or lessee of the computer; and (c) the specified person has relevant knowledge of: (i) the computer or a computer network of which the computer forms a part; or (ii) measures applied to protect data held in, or accessible from, the computer".

Although the privilege against self-incrimination was introduced in the Australian legislation in section 128 of the Evidence Act 1995[19], section 3LA of the aforementioned law explicitly provides that the order of the magistrate may be given to the suspected person, and thus the latter is not protected in this particular case. However, Australian jurisprudence seems to exempt suspects from section 3LA and thus protects them from decryption obligation[20].

---

18 Koops B. J. (2012), *The Decryption Order and the Privilege Against Self-Incrimination. Do developments since 2000 suggest a need to force suspects to decrypt?*, NCJ 242369, p. 179. For the Summary of the report in English, see the author's website http://www.cryptolaw.org/cls2.htm

19 Koops B. J. at http://www.cryptolaw.org/cls2.htm and http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/s128.html

20 According to Hocking B. A. and Manville L. L. (2001), *What of the right to silence: Still supporting the presumption of innocence, or a growing legal fiction?*, Macquarie Law Journal (2001) Vol 1 No 1, p. 76 "Under s 128(5) the court may require a witness to give evidence in circumstances where the answer is potentially incriminating.

2.3. Jurisprudential treatment of the phenomenon

Jurisprudential treatment of mandatory key disclosure presents a particular interest within this paper firstly because it allows us to examine its treatment in practice and also due to the important role that courts' decisions play in forming the characteristics of both compelled decryption and the privilege against self-incrimination.

With reference to the basic characteristics of the privilege against self-incrimination jurisprudence has formed a quite consistent view of it. Thus, one of the fundamental characteristics recognized by the courts is that the encryption password does not constitute a material which "has an existence independent of the will of the suspect" (Ashworth A. 2008:773) as the court stated in the Saunders case and as such falls within the protection of the privilege[21]. The important factor in the above material lies within the notion of compulsion, as it is regarded "that the exercise of those compulsory powers requires no co-operation from the suspect, whereas compulsion to speak or to hand over documents operates directly on the suspect's mind" (*idem*).

It is obvious that this direct compulsion is exactly what takes place in case of compelled decryption of a password[22] while the force to obtain blood or hair samples does not violate the privilege[23]. It is argued though that "this rationale [...] seems to be little more than an exercise of

---

However, by giving the witness a certificate (s 128(6)) and ensuring that the evidence may not be used in other proceeding against the witness (s 128(7)), the privilege against self- incrimination is complied with'.

21 In Saunders the Court stated that "The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing". (Ashworth A. 2008, Self-incrimination. In European Human Rights Law – A pregnant pragmatism?, Cardozo law review, vol. 30, no. 3Cardozo law review, vol. 30, no. 3, p. 758)

22 In modern technology the notion of a password is wider and it may include elements that used to be regarded as belonging to material not depended on the will of the suspect. As Goldman K., referring to the US legislation, notes (2011, *Biometrics password and the privilege against self-incrimination, Cardozo Arts & Entertainment,* Vol. 33, p. 18) "if a traditional alphabetic or numeric password, stored in the mind of its owner, is entitled to constitutional protection, then its modern technological counterpart m should receive similar constitutional safeguards. The compulsion of a suspect by law enforcement to unlock an iPhone or similar device through the use of his fingerprint falls well within the scope of rights afforded by the Fifth Amendment privilege against self-incrimination, and furthers the policy goals espoused by the Fifth Amendment".

23 Goldman K. (2011), B*iometrics password and the privilege against self-incrimination, Cardozo Arts & Entertainment,* Vol. 33, p. 16 where "The barriers to obtaining a suspect's fingerprints are relatively low because

ingenuity in order to defend a practice that can be justified only on pragmatic grounds" (Ashworth A. 2008:773).

Another significant characteristic of the privilege against self-incrimination relates to the seriousness of the offence and the public interest. In Saunders v. UK in 1996 the European Court of Human Rights (ECtHR) rejected the "argument that the complexity of corporate fraud and the vital public interest in the investigation of such fraud and the punishment of those responsible could justify such a marked departure as that which occurred in the present case from one of the basic principles of a fair procedure" (Trechel S. 2005:345). It is clear that according to the Court neither the seriousness of the crime nor the public interest can justify a compelled password decryption in case the privilege against self-incrimination protects the suspect. However, this position of the Court was later reversed as we shall see in several cases.

Furthermore, in the case K. v. Austria of 1992 the Commission insisted on the significance of the privilege against self-incrimination and noted "that the principle of protection against self-incrimination is, like the principle of presumption of innocence, one of the most fundamental aspects of the right to a fair trial". In this case the Commission applied the negative aspect of Article 10 and came to the conclusion "that the right to freedom of expression by implication also guarantees a "negative right" not to be compelled to express oneself, i.e. to remain silent". The Commission interpreted this right in the light of Article 6 and extended its application to people who are not accused or suspected of committing an offence but may be called to testify as a witness. Thus, the privilege of the person not to make a self-incriminatory statement is of a greater importance in its role to guarantee a fair trial than "a legitimate aim in conformity with the Article 10 par. 2, and a pressing social need for the compulsion – such as the duty to testify as a witness" (*Ibid*. 2005:343).

However, John Murray v. UK in 1996 was the first case which concerns legislation permitting inferences from the silence of a suspect under certain circumstances[24]. According to the Commission

---

compelling a suspect to provide law enforcement officials with his fingerprint is not considered to be an intrusion on something that is personal to the individual; rather, it is considered to be a freely available method of identification, akin to a photograph".

24 It is noteworthy that "The right to silence is the right of a suspect to say nothing in the face of police questioning and is justified as a protection from self-incrimination. The second tier to the right to remain silent concerns the right not to have silence used against one at trial". (Hocking B. A. and Manville L. L. (2001), *What of the right to silence: Still supporting the presumption of innocence, or a growing legal fiction?*, Macquarie Law Journal (2001) Vol

"whether a particular applicant has been subject to compulsion to incriminate himself in such a way as to render the criminal proceedings unfair ... will depend on an assessment of the circumstances of the case as a whole".

Furthermore, the Court stated that "on the one hand, it is self-evident that it is incompatible with the immunities under consideration to base a conviction solely or mainly on the accused's silence or on a refusal to answer questions or to give evidence himself. On the other hand, the Court deems it equally obvious that these immunities cannot and should not prevent that the accused's silence, in situations which clearly call for an explanation from him, be taken into account is assessing the persuasiveness of the evidence adduced by the prosecution. Wherever the line between these two extremes is to be drawn, it follows from this understanding of "the right to silence" that the question whether the right is absolute must be answered in the negative" (Trechel S. 2005:345).

The above conclusion reverses fully that reached in Saunders v. UK where the Court had stated that "It cannot be compatible with the spirit of the Convention that varying degrees of fairness apply to different categories of accused in criminal trials. The right of silence, to the extent that it may be contained in the guarantees of Article 6, must apply as equally to alleged company fraudsters as to those accused of other types of fraud, rape, murder or terrorist offences. Further, there can be no legitimate aim in depriving someone of the guarantees necessary in securing a fair trial". The Court also stressed that "the right not to incriminate oneself cannot reasonably be confined to statements of admissions of wrongdoing or to remarks which are directly incriminating. Testimony obtained under compulsion which appears on its face to be of a non-incriminating nature – such as exculpatory remarks or mere information on questions of fact – may later be deployed in criminal proceedings in support of the prosecution case [...] It follows that what is of the essence in this context is the use to which evidence obtained under compulsion is put in the course of the criminal trial" (*Ibid*. 2005:344).

In a more recent decision in Allan v. United Kingdom (5 November 2002) the Court added several conditions that have to be born in mind while examining whether there is a violation of the right. Thus, “In examining whether a procedure has extinguished the very essence of the privilege against self-incrimination, the Court will examine the nature and degree of the compulsion, the

1 No 1, p. 65

existence of any relevant safeguards in the procedures and the use to which any material so obtained is put" (Ashworth A. 2008:763-4).

The above conditions were taken into consideration in Jalloh v. Germany in 2006 where according to the judgment "In order to determine whether the applicant's right not to incriminate himself has been violated, the Court will have regard, in turn, to the following factors: the nature and degree of compulsion used to obtain the evidence; the weight of the public interest in the investigation and punishment of the offence at issue; the existence of any relevant safeguards in the procedure; and the use to which any material so obtained was put" (*Ibid*. 2008:765). The problem that arises in this case is that the judgment adds explicitly public interest as one of the factors affecting the application of the privilege against self-incrimination and secondly it implies that the seriousness of the offence also has to be taken into consideration. As it is noted "Insofar as the Court held that a minor drug-dealing case was not sufficiently weighty to justify overriding the privilege against self-incrimination, does this mean that the decisions in Saunders (on serious fraud) and in Heaney and McGuinness (on terrorism) are now open to doubt?" (*Ibid*. 2008:766-7).

Finally two more notions present particular significance considering the criminal procedure and the respect of the privilege against self-incrimination. The first one is related to the way in which the compulsion exercised by the authorities and has been an issue in several cases. More specifically, "The notion that putting a 'single, simple question' made the violation of the privilege against self-incrimination more acceptable was articulated by Lord Bingham in the Privy Council in Brown v. Stott and adopted by the Strasbourg Court in Weh v. Austria and in O'Halloran and Francis v. United Kingdom ("markedly more restricted" information)" (*Ibid*. 2008:771). On the other hand, this issue was not considered relevant by the Court in Heaney and McGuinness v. Ireland, that is that whether the suspects were requested to give a full account for their movements at a specific time or simply asked if they were in the specific place, the application of the privilege would not be affected (*Idem*).

The second notion relates to the term "the duty to self-identify" which is "a duty frequently imposed by the British legislature, in a whole range of situations" (*Ibid*. 2008:769). In these cases it has been proposed that the privilege against self-incrimination needs to be violated in order to secure the public interest. However, as Ashorth A. notes "It is unpersuasive to argue that the degree of violation of the privilege against self-incrimination in such cases should be "balanced" against the

public interest in road safety or in securing the conviction of those who breach the rules of the road. ...So the "balancing" approach is unsatisfactory, because it is incompatible with proper respect for those human rights that are not qualified on the face of the Convention" (*Idem*). It is clear that the same applies to compelled key decryption related to the identity of the suspect[25].

Chapter 3: Comparative analysis

After an extensive reference to both legislation in several countries and jurisprudence that have played a significant role in forming the privilege against self-incrimination in case of compelled key decryption we consider it of great importance to attempt to compare the above in order to obtain a clear of the current trends in the field.

3.1 Comparison of the above legal orders

Comparing the legal orders examined in the previous chapters concerning the protection of the individuals from compelled data decryption allows us to draw several interesting conclusions on the

25 As Goldman K. (2011), *Biometrics password and the privilege against self-incrimination, Cardozo Arts & Entertainment,* Vol. 33, p. 23, notes with relation to the US jurisprudence "In In re: Grand Jury Subpoena Duces Tecum, the Court of Appeals ultimately held that compelling the suspect to use an encryption password was analogous to using the contents of his mind, subsequently making the production of the unencrypted contents of the hard drives m testimonial. The court determined that "the decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files".

issue.

First of all, with reference to compelled decryption all of the examined legislations include provisions according to which authorized officials may require the disclosure of encrypted data that are of interest in a specific case and this requirement may be addressed to any person that is regarded to have the necessary technological knowledge in order to provide access to the encrypted data. That is to say that investigatory authorities may use any means that they dispose of with a view to gain access to encrypted data and obtain evidence related to an offence. In most legislations, the relevant provisions relate to laws that deal with cybercrime and terrorism. Nevertheless, since the burden of proof lies on the prosecution and not on the suspect, a principle which is reflected in the presumption of innocence and the right to silence, the individual is protected[26] by the privilege against self-incrimination and thus may not provide the disclosure key or disclose themselves the encryption password.

In the above examined legal orders though we noticed that in most of them the privilege against self-incrimination is not explicitly provided but only implied. Thus, with the exemption of the Australian legal order where it is explicitly provided that the suspect may be forced to produce the decryption key and thus provide self-incriminating information, the privilege against self-incrimination is expressly provided in the Civil Evidence Act 1968 in UK, and only implied in the legal orders of France, Belgium and Netherlands.

However, individuals of the above countries, apart from Australian citizens since Australia is not a member of the Council of Europe, may recourse to the protection provided by Art. 6 of the ECHR and take a case to the ECtHR when they feel that their privilege against self-incrimination has been violated.

---

26 According to Clemens A. M. 2008, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, Computer Crime Seminar Georgetown University Law Center Professors Richard Salgado 3 & Christian Genetski, p. 8 "The Murphy Court recognized that the privilege may sometimes be "a shelter to the guilty" but that it is "often a protection to the innocent. The Murphy Court, with no dissent, found the privilege justified the privilege for numerous reasons, including its "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt".

3.2 Comparison of the jurisprudential trends

As we have seen not all judgments have applied the privilege against self-incrimination in the same way. While some of them have recognized an absolute power of the privilege and given a wide notion to it others have added restrictions in its application.

Thus, in Funke v. France the Court recognized that "the privilege could not simply be balanced against the public interest in order to determine whether there had been a violation" (Ashworth A. 2008:753). Also, in Saunders the Court, even though it avoided to make a statement as to whether the privilege against self-incrimination in absolute or not, concluded that the privilege should "apply to criminal proceedings in respect of all types of criminal offences without distinction from the most simple to the most complex". Another significant judgment is the one in Heaney and McGuinness v. Ireland where according to the Court "the security and public order concerns of the Government cannot justify a provision which extinguishes the very essence of the applicants' rights to silence and against self-incrimination guaranteed by Article 6(1) of the Convention".

Furthermore, the Court asserted the importance of the privilege in the case Allan v. United Kingdom where "The right, which the Court has previously observed is at the heart of the notion of a fair procedure, serves in principle to protect the freedom of a suspected person to choose whether to speak or to remain silent when questioned by the police", as well as in the case K. v. Austria of 1992 which we mentioned in the previous chapter.

On the other hand, in the case John Murray v. United Kingdom the Court stated that the right to silence, and thus the privilege against self-incrimination, is not absolute and inferences[27] from a defendant's silence may be drawn by the Court in certain cases which depends on the "nature of the

27 Trechsel S. (2005), *Human Rights in Criminal Proceedings*, Oxford University Press, p. 346 "The direct aspect of the right concerns the situation of the person who is expected to give some sort of reaction to questions or requests. At its extreme, this means that it is definitely forbidden to have any recourse to torture in order to obtain a statement, whether self-incriminating or not. The indirect aspect concerns the use of any material obtained in violation of the right not to be compelled to make a statement, including the drawing of adverse inferences from the silence of an accused".

circumstances" (*Ibid*. 754). Moreover, restrictions have been recognized in the recent decisions in Allan v. United Kingdom and Jalloh v. Germany. We notice thus that while in first dealing with the issue the Court would seem more willing to recognize a violation in the privilege against self-incrimination and accept rare ad specifically justified divergences from it, in more recent cases restrictions have been added weakening the protection that is guaranteed by the privilege.

Finally, it is noteworthy that in several cases the nature of the offence has affected the conclusion of the Court. Thus, in O'Halloran and Francis v. United Kingdom the Grand Chamber implicitly took into account "the special nature of the regulatory regime" (Ashworth A. 2008:763) that concerns road traffic law and concluded that there was no violation of the privilege against self-incrimination. The same conclusion was reached by the Court in Weh v. Austria. In both cases the justification was that there had not been a direct compulsion to provide self-incriminating information but that there was asked just a simple question.

3.3 Guaranteeing the balance between the rights in conflict

By examining the above mentioned legislation and jurisprudence it is clear that both legislative bodies and courts meet the necessity to balance rights in conflict.

Thus, on one hand there are numerous collective and individual rights and principles within criminal law such as the public interest, road safety, national security which need to be guaranteed. What is more, the prosecution and compulsory powers bear the burden to obtain the necessary evidence to support the charge in order to unravel a crime.

However, respect of human rights within criminal proceedings is equally important since the individual is particularly vulnerable against the state and the judicial bodies. In this context, the privilege against self-incrimination constitutes a fundamental right in protecting individuals from a possible access to personal and sensitive data, from the compulsion to choose between lying and witnessing against themselves, from the drawing of adverse inferences from their silence. As noted by Ashworth (2008:768) "the privilege against self-incrimination and the right of silence belong to a cluster of criminal justice rights, centering on the presumption of innocence and the principle of equality of arms, and reaching out to the right of confidential access to a legal adviser, the right to disclosure of evidence held by the prosecution, the right of confrontation and other rights expressed in or implied into Article 6 of the Convention." We have seen that the Court has made more or less successful efforts to balance the rights in conflict. In recent decisions it has concluded that the privilege against self-incrimination is not absolute and several restrictions have been added to its application. Even if we accept the fact that in certain situations there may be justifiable exceptions from the privilege, it is important that these are clear and do not violate fundamental rights such as the rule of law and equality of citizens before the law.

Conclusions

Data encryption and decryption as well as the passwords produced to encrypt and decrypt information are an integral part of modern society where a significant amount of information personal or professional is stored and delivered in a digital form. Thus, legislation that regulated both encryption and decryption has made its appearance in a national and international level.

In criminal proceedings compelled production of passwords rises the application of conflicting rights that need to be balanced. On the one hand stands the "right" and obligation of the state and the judicial bodies to investigate and unravel a criminal act in order to enforce order through the punishment of the criminal. On the other hand, ensuring the human rights of the suspect and the person charged with a crime constitute a fundamental aspect of the rule of law and of the right to a fair trial. The privilege against self-incrimination has been recognized implicitly or expressly in numerous national legislations and international treaties. It is also regarded as a significant part of the presumption of innocence which guarantees that the burden of proof lies on the prosecution and the suspect cannot be compelled to choose between witnessing against themselves and committing perjury. Thus, in the legal orders examined in this dissertation investigatory powers may request the production of decryption keys from persons regarded as capable of meeting the requirement and generally make any lawful effort in order to obtain evidence that concern a crime but this request cannot be made to the person charged with a crime.

Moreover, we have seen that jurisprudence has generally formed in practice the privilege against self-incrimination in cases concerning access of the authorities to possible self-incriminating information. Although it has recognized the importance of the privilege as a human right numerous restrictions introduced in certain cases may have loosen its power confirming its non-absolute character. Possible exceptions from the privilege though have to be accepted only in rare situations and with clear criteria which do not violate fundamental human rights.

Bibliography

Andrews S. (2000), *Use Who Holds the Key? - A Comparative Study of US and European Encryption Policies*, JILT 2000 (2)

Ashworth A. (2008), *Self-incrimination. In European Human Rights Law – A pregnant pragmatism?*, Cardozo law review, vol. 30, no. 3

Clemens A. M. (2004), *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, Computer Crime Seminar Georgetown University Law Center Professors Richard Salgado 3 & Christian Genetski

Comprehensive Study on Cybercrime, Draft-February 2013, United Nations Office On Drugs and Crime

Goldman K. (2011), *Biometrics password and the privilege against self-incrimination, Cardozo Arts & Entertainment*, Vol. 33

Hocking B. A. and Manville L. L. (2001), *What of the right to silence: Still supporting the presumption of innocence, or a growing legal fiction?*, Macquarie Law Journal (2001) Vol 1 No 1

Kahn D. (1996), *The Codebreakers: The Story of Secret Writing*, Scribner, New York

Kaspersen H. W. K. (2004),

Koops B. J. (2010), *Cybercrime Legislation in the Netherlands,* Electronic Journal of Comparative Law, vol. 14.3, December 2010

Koops B. J. (2012), *The Decryption Order and the Privilege Against Self-Incrimination. Do developments since 2000 suggest a need to force suspects to decrypt?*, NCJ 242369

Mandelman J. C. (1998), *Lest We Walk Into The Well: Guarding the Keys—Encrypting the Constitution: To Speak, Search & Seize in Cyberspace*, 8 Alb. L. J. Sci. & Tech.

Rueda A. (2001), *The Implications of Strong Encryption Technology on Money Laundering*, 12 Alb. L.J. Sci. & Tech.

Saper N. (2013), *International Cryptography Regulation and the Global Information Economy*, Northwestern Journal of Technology and Intellectual Property, Vol. 11, Issue 7

Shackleford D., (2007), *Regulations and Standards: Where Encryption Applies*, SANS Institute InfoSec Reading Room, November 2007

Trechsel S. (2005), *Human Rights in Criminal Proceedings*, Oxford University Press

Web Sources

(All last accessed on 13/02/2016)

http://cwisdb.kuleuven.be/pisa/fr/jur/infocrimewet.htm http://www.legislation.gov.uk/ukpga/2000/23/part/III

http://www.austlii.edu.au/au/legis/cth/bill_em/cb2001122/memo1.html

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052

http://www.legislation.gov.uk/ukpga/1968/64/section/14

http://www.legislation.gov.uk/ukpga/2006/35/section/13

http://www.cryptolaw.org/cls2.htm

http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/s128.html